Approximate Quantum Error-Correcting Codes and Secret Sharing Schemes

Claude Crépeau[1] *, Daniel Gottesman[2] **, and Adam Smith[3] ***

[1] McGill University, Montréal, QC, Canada. crepeau@cs.mcgill.ca
[2] Perimeter Institute, Waterloo, ON, Canada. dgottesman@perimeterinstitute.ca
[3] Weizmann Institute of Science, Rehovot, Israel. adam.smith@weizmann.ac.il

Abstract. It is a standard result in the theory of quantum error-correcting codes that no code of length n can fix more than $n/4$ arbitrary errors, regardless of the dimension of the coding and encoded Hilbert spaces. However, this bound only applies to codes which recover the message exactly. Naively, one might expect that correcting errors to very high fidelity would only allow small violations of this bound. This intuition is incorrect: in this paper we describe quantum error-correcting codes capable of correcting up to $\lfloor (n-1)/2 \rfloor$ arbitrary errors with fidelity exponentially close to 1, at the price of increasing the size of the registers (i.e., the coding alphabet). This demonstrates a sharp distinction between exact and approximate quantum error correction. The codes have the property that any t components reveal no information about the message, and so they can also be viewed as error-tolerant secret sharing schemes.

The construction has several interesting implications for cryptography and quantum information theory. First, it suggests that secret sharing is a better classical analogue to quantum error correction than is classical error correction. Second, it highlights an error in a purported proof that verifiable quantum secret sharing (VQSS) is impossible when the number of cheaters t is $n/4$. In particular, the construction directly yields an *honest-dealer* VQSS scheme for $t = \lfloor (n-1)/2 \rfloor$. We believe the codes could also potentially lead to improved protocols for dishonest-dealer VQSS and secure multi-party quantum computation.

More generally, the construction illustrates a difference between exact and approximate requirements in quantum cryptography and (yet again) the delicacy of security proofs and impossibility results in the quantum model.

* Supported in part by Québec's MDER, FQRNT, Canada's NSERC, MITACS, CIAR and the Bell University Laboratories. Some of this research was done while the author was visiting MSRI, Berkeley CA.
** Some of this research was done while the author was supported by the Clay Mathematics Institute, and some while the author was visiting MSRI, Berkeley CA.
*** Some of this research was done while the author was a student at the MIT CSAIL.

1 Introduction

Quantum computers are likely to be highly susceptible to errors from a variety of sources, much more so than classical computers. Therefore, the study of quantum error correction is vital not only to the task of quantum communications but also to building functional quantum computers. In addition, quantum error correction has many applications to quantum cryptography. For instance, there is a strong connection between quantum error-correcting codes and secret sharing schemes [6], and that connection was combined with fault-tolerant quantum computation to perform multiparty secure quantum computations [9]. Many quantum key distribution schemes also rely on ideas from quantum error-correction for their proofs of security. Thus, bounds on the performance of quantum error-correcting codes (QECCs) in various scenarios are relevant both to the foundations of quantum information theory and to quantum cryptography.

It is an immediate result of the no-cloning theorem [24] that no quantum error-correcting code of length n can fix $n/2$ erasures: such a code would allow one to reconstruct two copies of an encoded quantum state from two halves of the full codeword, which would be cloning the state. This result is valid regardless of the dimension of the coding Hilbert space. Another well known result from the theory of quantum error correction is that a length n code can fix t arbitrary single position errors if and only if it can fix $2t$ erasure errors [11]. This follows immediately from the quantum error-correction conditions [11]

$$\langle \psi_i | E_a^\dagger E_b | \psi_j \rangle = C_{ab} \delta_{ij} \tag{1}$$

(for basis encoded states $\{|\psi_i\rangle\}$ and correctable errors $\{E_a\}$) and implies that no QECC of length n can fix more than $n/4$ arbitrary errors, regardless of the dimension of the coding and encoded Hilbert spaces. In contrast, a classical repetition code can correct up to $\lfloor (n-1)/2 \rfloor$ errors.

In this paper, we describe QECCs of length n that can correct arbitrary errors which affect up to $t = \lfloor (n-1)/2 \rfloor$ positions, with the guarantee that the fidelity of the reconstructed state will be exponentially close to 1. That is, *approximate* quantum error-correcting codes have the capability of correcting errors in a regime where no *exact* QECC will function. The scheme is also a secret-sharing scheme, in that no t positions reveal any information at all about the message. The result has a number of implications for both cryptography and quantum information theory:

- It may be possible to build approximate QECCs which are highly efficient and yet useful in common error correction scenarios, improving on exact QECCs for the same scenarios. In most cases, exact reconstruction of the quantum state is not necessary, so a more efficient approximate QECC would be welcome.
- The connection between correcting general errors and erasure errors breaks down for approximate QECCs. This suggests there is no sensible notion of distance for an approximate quantum error-correcting code.

- The proof of the impossibility of *verifiable quantum secret sharing* (VQSS) with $t \geq n/4$ cheaters in [9] is incorrect, since it assumes that the $t < n/4$ bound on error correction extends to approximate quantum codes. In particular, the construction described here immediately yields an honest-dealer verifiable quantum secret sharing scheme which is secure for $t = \lfloor (n-1)/2 \rfloor$. Similar constructions may allow verifiable quantum secret sharing (VQSS) with a *dishonest* dealer and secure multiparty quantum computation (MPQC) beyond previously known bounds. We have devised candidate protocols for these tasks allowing up to $(n-1)/2$ cheaters, but we do not present them here, as we have not yet proved their security and they are, in any case, quite complex.
- Secret sharing may serve as a better classical analogue to quantum error correction than does classical error correction. The sharp difference we see between perfect and approximate quantum error correction parallels to some extent a similar difference between error-tolerant secret sharing schemes (explained below) with zero error and those with exponentially small error [19]. The codes here use such secret sharing schemes as a building block.
- More generally, our results demonstrate that there can be a dramatic difference in behavior between the exact performance of some quantum-mechanical task and approximate performance of the task, even when the approximation is exponentially good. A similar divergence between exact and approximate bounds has recently been seen in the context of private quantum channels [13]. These examples serve as a caution — especially valid in cryptography — that intuition about approximate performance of quantum protocols may be misleading.

The idea of using a randomized encoding algorithm is not new in QECC. In particular [4] have devised codes that can correct more (malicious) errors on average than any deterministic QECC. However, their model significantly differs from ours in one of two ways: they assume either that the errors occur at random or that the code is randomly agreed on by the coder and the decoder but is kept secret from the adversarial noise source. This model does not seem suitable in cryptographic applications such as VQSS and MPQC [9]. In our model no secret is shared by the coder and decoder. However, part of our code can be viewed as providing a way for the coder to information-theoretically encrypt the necessary secret. (This is possible since the adversary only has access to part of the transmitted state, though it could be any part.)

A closer analogue to our codes is present in [15], which gave a pure-state encoding to approximately correct a specific error model more efficiently than a typical minimum-distance code. (Note, however, that the nature of the error model in fact precludes *any* exact quantum error-correcting code.) Closer yet is [21], which considered approximate quantum error correction in precisely our sense, and studied conditions for approximate error correction to be possible. They did not, however, present any specific codes or suggest that approximate QECCs might allow significant improvements in the number of correctable registers.

Secret Sharing and Quantum Error Correction Classically, an (n, d)-secret sharing scheme splits a secret into n pieces so that no $d-1$ shares reveal any information about the secret, but any d shares allow one to reconstruct it. Such a scheme is already an error-correcting code, since it allows one to correct up to $n-d$ erasures. Error-correcting codes need not be secret sharing schemes: a repetition code, for example, provides no secrecy at all. In the quantum world, the connection is much tighter. Cleve *et al.* [6] observed that any (perfect) QECC correcting t erasures is itself a secret sharing scheme, in that no t components of the code reveal any information about the message. This follows from the principle that information implies disturbance. Furthermore, most known (perfect) classical secret sharing schemes (and "ramp" schemes) can be directly transformed into (perfect) QECC's with the related parameters [22].

The quantum code construction described here illustrates a further connection to classical secret sharing. An error-tolerant secret sharing scheme (ETSS) can recover the secret even when t shares have been maliciously corrupted. Ordinary (n, d)-secret sharing schemes are error-tolerant: such a scheme corrects $n - d$ erasures and hence $t = (n - d)/2$ errors (this fact was first highlighted for Shamir secret sharing in [16]). If we also want any t shares to reveal no information, then we get $t < d$, and thus $t < n/3$. This is optimal for schemes with zero error probability. On the other hand, if one allows a small probability of mistaken error correction, then one can in fact get error-tolerant secret sharing schemes which correct $t = \lfloor (n-1)/2 \rfloor$ errors (see the Preliminaries for more details). Thus, the best classical analogue for approximate quantum codes are error-tolerant classical secret sharing schemes which correct any t errors with high probability. These have been studied more or less explicitly in work on multi-party computation [19, 7, 8].

It is worth noting that the construction of quantum error-tolerant secret sharing schemes has farther reaching implications than analogous classical constructions. Our approximate quantum codes correct a number of general errors for which no exact code would suffice, whereas the classical constructions can be better understood as reducing the number of erasures that can be corrected via secret sharing techniques. A straightforward classical repetition code already corrects up to $\lfloor (n-1)/2 \rfloor$ arbitrary errors exactly, so there is no need to resort to sophisticated techniques to achieve this with classical ECCs.

Results Our construction produces quantum codes which encode ℓ qubits into n registers of $\frac{\ell}{(n-2t)} + O(ns)$ qubits each and which correct any t adversarial errors with probability 2^{-s} (the bound assumes $\log n < \ell < 2^s$ for simplicity). This is done by transforming $[[n, 1, n/2]]_n$ QECCs on n-dimensional registers into better codes on $2^{O(ns)}$-dimensional registers. The codes we construct are always decodable in polynomial time, since the only necessary operations are verification of quantum authentication and erasure correction for a stabilizer code, and since erasure correction for a stabilizer code only requires solving a system of linear equations.

2 Preliminaries

Classical Authentication For our purposes, a classical (one-time) authentication scheme is a function $h_a(m)$ that takes a secret key a and a message m as input (and no other randomness), and outputs a tag for the message. Typically, Alice sends the pair $m, h_a(m)$ to Bob, with whom she shares the key a. Bob receives a pair m', tag' and accepts the message as valid if and only if $tag' = h_a(m')$. Bob will always accept a message that really came from Alice. The scheme has error ϵ if, given a valid pair $m, h_a(m)$, no adversary Oscar can forge a tag for a different message m' with probability better than ϵ. That is, for all messages m and all (computationally-unbounded, randomized) algorithms $O()$, if a is chosen randomly from a set of keys $\mathcal{K}$, then:

$$\Pr_{a \leftarrow \mathcal{K}}[m', tag' \leftarrow O(m, h_a(m)) \ : \ tag' = h_a(m')] \leq \epsilon.$$

We make no assumptions on the running time of the adversary. If the message is ℓ bits long, then one can find a polynomial time authentication scheme where both the key and the tags have length $O(\log \ell + \log(\frac{1}{\epsilon}))$ (see, e.g., [10]).

For the remainder of this paper, we assume the reader is familiar with the basic notions and notation of quantum computing (see a textbook such as [17] if necessary).

Quantum Authentication Intuitively, a quantum authentication scheme [2] is a keyed system which allows Alice to send a state ρ to Bob with a guarantee: if Bob accepts the received state as "valid", the fidelity of that state to ρ is almost 1. Moreover, if the adversary makes no changes, Bob always accepts and the fidelity is exactly 1. The following definition is from Barnum et al. [2]. We first define what constitutes a quantum authentication scheme, and then give a definition of security.

Definition 1 ([2]) *A* quantum authentication scheme *(*QAS*) is a pair of polynomial time quantum algorithms A and V together with a set of* classical *keys $\mathcal{K}$ such that:*

- *A takes as input an m-qubit message system M and a key $k \in \mathcal{K}$ and outputs a transmitted system C of $m + t$ qubits.*
- *V takes as input the (possibly altered) transmitted system $\hat{C}$ and a classical key $k \in \mathcal{K}$ and outputs two systems: a m-qubit message state $\hat{M}$, and a single (verdict) qubit V which indicates acceptance or rejection. The classical basis states of V are called $|\text{ACC}\rangle, |\text{REJ}\rangle$ by convention.*

For any fixed key k, we denote the corresponding super-operators by A_k and V_k.

Bob may measure the qubit V to see whether or not the transmission was accepted or rejected. Nonetheless, we think of V as a qubit rather than a classical bit since it will allow us to describe the joint state of the two systems $\hat{M}, V$ with a density matrix. Given a pure state $|\psi\rangle \in \mathcal{H}_M$, consider the following test on

the joint system $\hat{M}, V$: output a 1 if the first m qubits are in state $|\psi\rangle$ *or* if the last qubit is in state $|\text{REJ}\rangle$ (otherwise, output a 0). The projectors corresponding to this measurement are

$$P_1^{|\psi\rangle} = |\psi\rangle\langle\psi| \otimes |\text{ACC}\rangle\langle\text{ACC}| \ + \ I_{\hat{M}} \otimes |\text{REJ}\rangle\langle\text{REJ}|$$
$$P_0^{|\psi\rangle} = (I_{\hat{M}} - |\psi\rangle\langle\psi|) \otimes (|\text{ACC}\rangle\langle\text{ACC}|)$$

We want that for all possible input states $|\psi\rangle$ and for all possible interventions by the adversary, the expected fidelity of V's output to the space defined by $P_1^{|\psi\rangle}$ is high. This is captured in the following definition of security.

Definition 2 ([2]) *A* QAS *is secure with error ϵ for a state $|\psi\rangle$ if it satisfies:*

- Completeness: *For all keys $k \in \mathcal{K}$: $V_k(A_k(|\psi\rangle\langle\psi|)) = |\psi\rangle\langle\psi| \otimes |\text{ACC}\rangle\langle\text{ACC}|$*
- Soundness: *For a super-operator $\mathcal{O}$, let ρ_{Bob} be the state output by Bob when the adversary's intervention is characterized by $\mathcal{O}$, that is: $\rho_{Bob} = \frac{1}{|\mathcal{K}|}\sum_k V_k(\mathcal{O}(A_k(|\psi\rangle\langle\psi|)))$ (this is the expectation over all values of the key of the state output by Bob). The* QAS *has soundness error ϵ for $|\psi\rangle$ if for all super-operators $\mathcal{O}$,*

$$\text{Tr}\left(P_1^{|\psi\rangle}\rho_{Bob}\right) \geq 1 - \epsilon$$

A QAS *is secure with error ϵ if it is secure with error ϵ for all states $|\psi\rangle$. We make no assumptions on the running time of the adversary.*

In order to authenticate a message of ℓ qubits, the authentication scheme of [2] uses a (classical) key of length $2\ell + O(\log(\frac{1}{\epsilon}))$ random bits and produces a transmitted system of $\ell + O(\log(\frac{1}{\epsilon}))$ qubits. The large part 2ℓ of the classical key is used to the encrypt the quantum state, which is necessary for any quantum authentication scheme to be secure [2]. In the special case where Alice wishes to authenticate half of a maximally entangled state $\sum |i\rangle|i\rangle$, in fact only $O(\log(\frac{1}{\epsilon}))$ classical key bits are necessarily [18, 12], effectively because Alice's message is already a maximally mixed state, making encryption redundant.

Composability of Quantum Authentication We will need authentication protocols that have an additional composability property: If (A_k, V_k) is a QAS with error ϵ for key k, then the concatenated protocol

$$\left(\bigotimes_{i=1}^{n} A_{k_i}, \bigotimes_{i=1}^{n} V_{k_i}\right) \tag{2}$$

should be a QAS with error ϵ for the key $(k_1, \ldots, k_n)$, with the understanding that the concatenated verification protocol accepts if and only if all of the tensor components accept (i.e. the verdict qubit for the concatenated scheme is the logical AND of the individual verdict qubits).

This sort of composability holds trivially for a classical authentication scheme, although the error may increase linearly with the number of compositions. We

do not know if the same is true in general for quantum authentication schemes. However, the quantum authentication schemes of [2] are indeed composable, with no blow-up in the error parameter. This follows because they are constructed from stabilizer purity testing codes (PTCs), which clearly satisfy a corresponding property (if Q_k is a stabilizer PTC with error ϵ, then $\bigotimes_{i=1}^{n} Q_{k_i}$ is a stabilizer PTC with error ϵ).

Classical Secret Sharing and Error Correction A classical (n, d)-secret sharing scheme [20] is a cryptographic protocol allowing a *dealer* to share a secret k into n *shares* $(s_1, \ldots, s_n)$ with n *share-holders* $P_1, \ldots, P_n$ in such a way that any $d-1$ s_i's contains no information about k whereas any d of those s_i's completely define k. We write $(s_1, \ldots, s_n) \in_R SS_{n,d}(k)$, a random instantiation of a set of shares for secret k. The original construction of Shamir [20], based on Reed-Solomon codes, allows one to share an ℓ-bit secret with shares that are each $\max\{\ell, \log n\}$ bits.

An important component in our construction is a classical secret sharing scheme which allows the honest players to reconstruct the secret even if the cheaters alter their shares. Specifically, consider the following game: an honest dealer takes a secret, splits it into n shares $s_1, .., s_n$, and distributes the shares amongst n participants over secure channels (i.e., player i gets only s_i). Next, an adversary (adaptively) corrupts up to $t = d-1$ of the players. Finally, all players send their (possibly corrupted) shares over secure channels to a trusted arbiter who attempts to recover the secret. The secret sharing scheme is called an *error-tolerant secret sharing scheme* (ETSS) and is *t-error-correcting with error ϵ* if the arbiter can reconstruct the correct secret with probability $1 - \epsilon$, regardless of the adversary's strategy. In other words, an ETSS is a secret-sharing scheme which also acts as an error-correcting code correcting any t errors with high probability.

Error-tolerant secret sharing has been studied under the names "honest-dealer VSS with a non-rushing adversary" [8] and "non-interactive Las Vegas perfectly secure message transmission" [23]. "Robust secret sharing" [5] is a slightly weaker variant of the problem. Another variant, "honest-dealer VSS with rushing" is slightly stronger than ETSS; see [8] for a discussion of the differences.

A number of constructions of ETSS schemes appear in the literature. When $t < n/3$, any ordinary secret sharing scheme is in fact an ETSS with zero error (since it is a code correcting $2t$ erasures and hence t errors). This connection was first pointed out by [16]. When t is between $n/3$ and $n/2$, one can adapt constructions from multi-party computation protocols [19, 7, 8]. We will use a simple construction for the case $t = \lfloor (n-1)/2 \rfloor$ from [8]. The dealer encodes the secret using an ordinary secret sharing scheme, and augments the shares by creating a fresh authentication key and tag for every pair of players: P_i gets the key a_{ij} and P_j gets the tag $h_{a_{ij}}(s_j)$. If the adversary does not succesfully forge any authentication tags for keys held by honest players, then the arbiter can reconstruct the secret by accepting only shares for which at least $t + 1$ of the authentication tags are valid.

The two schemes suggested above tolerate the maximum number of cheaters. On one hand, schemes with zero error can tolerate at most $n/3$ errors [19]. On the other hand, it is clear that no ETSS scheme can correct more than $t = \lfloor (n-1)/2 \rfloor$ errors: any $n-t$ players must be able to reconstruct the secret alone (as the adversary could simply erase all its shares), and so we must have $n-t > t$. Alternatively, one can view this as an ordinary error correction bound: if the adversary could control half of the shares, he could make them all consistent with a value of his choosing (say 0) and force the arbiter to reconstruct 0.

The main complexity measure of an ETSS scheme is the share size. For a given scheme, let $CC(\ell, \epsilon, t)$ denote the maximum size (in bits) of a share held by any player. When $t < n/3$, the usual Shamir secret sharing scheme is a zero-error ETSS scheme with zero error and share size $CC(\ell, 0, t) = \ell/(n-3t)$ (for $\ell > (n-3t)\log n$). The errors can be corrected in polynomial time since the scheme encodes data in a Reed-Solomon code. For $t = \lfloor (n-1)/2 \rfloor$, the augmented scheme using authentication tags produces shares of size $CC(\ell) = \ell + O(n \log(\frac{1}{\epsilon}))$ (when $\ell > \log n$ and $\log(\frac{1}{\epsilon}) > \max\{n, \ell\}$).

Based on [5], Cramer et al. [8] present a more compact scheme for $t = \lfloor (n-1)/2 \rfloor$ with share size $O(\ell + n + \log(\frac{1}{\epsilon}))$. Unfortunately, that scheme is not known to correct the errors in polynomial time. A second scheme, for t further away from $n/2$, generates shares of size $CC(\ell, \epsilon, t) = \Omega(n \log(\frac{1}{\epsilon}) + \ell/(n-2t))$. The same work [8] also proved a simple lower bound on the share size of ETSS schemes: $CC(\ell, \epsilon, t) = \Omega(\log(\frac{1}{\epsilon}) + \frac{\ell}{(n-2t)})$. This bound is tight for $\log(\frac{1}{\epsilon}) > n$ and $n = 2t+1$.

3 Definition of Approximate Quantum Codes (AQECC)

An approximate quantum error-correcting code allows Alice to send a state ρ to Bob with the guarantee that if few enough errors occur in transmission, the fidelity of the state received by Bob to ρ will be almost 1.

Let $q = p^m$ and $Q = p^N$ for some prime p and integers m, N. We first define what constitutes an AQECC over $\mathbb{F}_Q$, and then give a definition of correctness. (Note that the definition makes sense over any alphabet, but we restrict to prime powers for simplicity).

Definition 3 *An* approximate quantum error correcting code *(AQECC) is a pair of quantum algorithms E (encoder) and D (decoder) such that:*

- *E takes as input a m-quqit message system M and outputs a (mixed state) codeword C of n quQits.*
- *D takes as input the (possibly altered) transmitted system $\hat{C}$ and outputs a m-quqit message state $\hat{M}$.*

In our constructions, both the encoding E and error-correction algorithm D run in polynomial time in the number of qubits of input.

We will define the correctness of an AQECC on pure states, but it follows from a result of Barnum, Knill and Nielsen ([3], Thm 2) that the output of the

AQECC also has high fidelity to an input which is mixed or part of an entangled state.

Given a pure state $|\psi\rangle \in \mathcal{H}_M$, consider the following test on the system $\hat{M}$: output a 1 if the first k quqits are in state $|\psi\rangle$ (otherwise, output a 0). The projectors corresponding to this measurement are

$$\begin{aligned} P_\psi &= |\psi\rangle\langle\psi| \\ P_\psi^\perp &= (I_{\hat{M}} - |\psi\rangle\langle\psi|) \end{aligned}$$

We want that for all possible input states $|\psi\rangle$ and for all possible interventions by the adversary, the expected fidelity of Bob's output to the space defined by P_ψ is high. This is captured in the following definition of correctness.

Definition 4 *An AQECC is t-correct with error ϵ for a state $|\psi\rangle$ if for all super-operators $\mathcal{O}$ acting on at most t quQits (that is, $\mathcal{O}$ can be written as $I_{n-t} \otimes \tilde{\mathcal{O}}_t$ for some partition of the system into $n-t$ and t quQits),*

$$\mathrm{Tr}\,(P_\psi \rho_{Bob}) \geq 1 - \epsilon,$$

where ρ_{Bob} is the state output by Bob when the adversary's intervention[4] is characterized by $\mathcal{O}$, that is:

$$\rho_{Bob} = D(\mathcal{O}(E(|\psi\rangle\langle\psi|))).$$

An AQECC is t-correct with error ϵ if it is t-correct with error ϵ for all states $|\psi\rangle$.

4 A length 3 quantum code approximately correcting one arbitrary error

We start with a small example, from a well known code. The code c corrects one erasure error:

$$\begin{aligned} |0\rangle &\to |000\rangle + |111\rangle + |222\rangle \\ |1\rangle &\to |012\rangle + |120\rangle + |201\rangle \\ |2\rangle &\to |021\rangle + |102\rangle + |210\rangle \end{aligned} \tag{3}$$

Let $H_1 \otimes H_2 \otimes H_3$ be the coding space of the original code

$$c|\psi\rangle \in H_1 \otimes H_2 \otimes H_3,$$

and let (A_k, V_k) be a quantum authentication scheme as constructed in [2].

We construct a three-component code c' as follows:

$$\begin{aligned} c'|\psi\rangle = &(A_{k_1}(H_1), k_2, k_3), \\ &(A_{k_2}(H_2), k_1, k_3), \\ &(A_{k_3}(H_3), k_2, k_1). \end{aligned} \tag{4}$$

[4] We make no assumptions on the running time of the adversary.

Let $H'_1 \otimes H'_2 \otimes H'_3$ be the coding space of the new code

$$c'|\psi\rangle \in H'_1 \otimes H'_2 \otimes H'_3$$

Note that k_1, k_2, and k_3 are random *classical* strings which we use as keys for the quantum authentication protocol A_k. Thus, the H'_is contain both quantum and classical information. Intuitively, we use the QAS to ensure that an adversary cannot change the quantum state of a single register without being detected; thus, we can transform general errors into erasure errors, allowing us to correct one faulty register out of three (no exact QECC can do this). Then we distribute the authentication keys among the three registers so that Bob can recover them. We must, however, do so in a way that prevents an adversary with access to a single register from either learning the key applying to her own register (which would allow her to change the quantum state) or from preventing reconstruction of the classical keys.

Theorem 1 *If A_k is a* QAS *secure with error ϵ then c' is a* 1*-correct AQECC with error prob.* $\mathrm{poly}(\epsilon)$*, correcting one arbitrary error.*

We omit the proof of this theorem, as in Section 5 we will prove a more general result.

4.1 Reconstruction

In all cases, the reconstruction has two phases. First we reconstruct the classical keys and use them to verify and decode the quantum authentications. This may result in discarding one register, but at least two remain, which is enough for the erasure-correcting code to recover the original encoded state. Consider the following cases:

- All k_i's agree in H'_1, H'_2, H'_3:
  Recover k_i from either $H'_j, j \neq i$, check that $A_{k_i}(H_i)$ properly authenticates H_i. If one authentication fails, ignore the improperly authenticated H_i and reconstruct the valid codeword as $c|\psi\rangle \in H_1 \otimes H_2 \otimes H_3$ using the erasure recovery algorithm from both $H_j, j \neq i$.
- Some H'_i disagrees with H'_j, H'_h on both keys k_h and k_j:
  Discard register i, which must be corrupted. Recover k_j from H'_h and k_h from H'_j, and decode the authentications $A_{k_j}(H_j)$ and $A_{k_h}(H_h)$ (which should both pass, since only one register can fail). Reconstruct the valid codeword as $c|\psi\rangle \in H_1 \otimes H_2 \otimes H_3$ using the erasure recovery algorithm from H_j and H_h.
- H'_i and H'_j disagree on key k_h, while H'_h agrees with everyone:
  Either register i or j is corrupt. Get k_i and k_j from H'_h and check that $A_{k_i}(H_i)$ properly authenticates H_i, and that $A_{k_j}(H_j)$ properly authenticates H_j. If neither fails, reconstruct the valid codeword as $c|\psi\rangle \in H_1 \otimes H_2 \otimes H_3$ using the erasure recovery algorithm from H_i and H_j. If one fails, say $A_{k_i}(H_i)$, then conclude register i is corrupt and recover k_h from H'_j, decode $A_{k_h}(H_h)$, and reconstruct the valid codeword as $c|\psi\rangle \in H_1 \otimes H_2 \otimes H_3$ using the erasure recovery algorithm from H_h and H_j.

Other cases cannot arise, since only one register can have been changed from the original encoding.

5 A general n-component approximate QECC family correcting up to $d-1 < n/2$ arbitrary errors

In order to generalize the above construction to cases with n registers, we need to systemize the distribution of the classical keys. Again, it is helpful to imagine that we are trying to defeat an adversary with access to $t < n/2$ components of the code. Recall that we needed two conditions: First, the adversary should not be able to learn the classical key for her register, but the receiver Bob should be able to reconstruct the keys. Second, the adversary should not be able to interfere with Bob's reconstruction of the keys.

These are precisely the properties of an ETSS. This suggests the following strategy for building a t-correct AQECC: encode $|\psi\rangle$ using a distance $t+1$ QECC, authenticate the n components using keys $\boldsymbol{k} = k_1, ..., k_n$, and then share $\boldsymbol{k}$ using a classical ETSS. The result could be considered to be a quantum ETSS (that is, an ETSS for quantum data). However, the ramifications of this construction for quantum data are more far-reaching than for the classical protocol. Not only does the quantum ETSS have potential cryptographic applications, but it demonstrates the possibility of exceeding the no-cloning bound on QECCs. Indeed, any QECC, exact or approximate, is in some sense a quantum ETSS — the ability to (approximately) correct erasures on a set of registers implies that an adversary with access to those registers can gain (almost) no information about the encoded data [21].

Let $\mathcal{Q}$ be a QECC that can correct $d-1 < n/2$ arbitrary erasure errors: $\mathcal{Q} = [[n, k, d]]$. Such a code can be constructed over sufficiently large dimension Q; for instance, use a polynomial quantum code [1]. The coding space of $\mathcal{Q}$ is defined as

$$\mathcal{Q}|\psi\rangle \in H_1 \otimes H_2 \otimes H_3 \otimes ... \otimes H_n.$$

We assume $\dim(H_1) = \dim(H_2) = ... = \dim(H_n)$.

We construct a new code $\mathcal{Q}'$ over larger Hilbert spaces that can correct $d-1 < n/2$ arbitrary errors except with small probability. Register i of the n-component code $\mathcal{Q}'$ contains the following:

$$\langle A_{k_i}(H_i), s_i, [a_{ij}(\forall j \neq i)], [h_{a_{ji}}(s_i)(\forall j \neq i)]\rangle, \tag{5}$$

where we have used the classical authentication scheme (in systematic form):

$$m, a \rightarrow (m, h_a(m)), \tag{6}$$

which has error ϵ, and $(s_1, \ldots, s_n) \in_R SS_{n,d}(k_1, \ldots, k_n)$, a secret sharing scheme such that any $d-1$ s_i's contains no information about $(k_1, \ldots, k_n)$ whereas any d of those s_i's completely define $(k_1, \ldots, k_n)$. The combination of classical secret sharing and classical authentication forms an ETSS [8], as described above; in fact, any ETSS would do.

For instance, the $n = 3$ case of this construction is as follows:

$$\begin{aligned} c'|\psi\rangle = &(A_{k_1}(H_1), s_1, [a_{12}, a_{13}], [h_{a_{21}}(s_1), h_{a_{31}}(s_1)]), \\ &(A_{k_2}(H_2), s_2, [a_{21}, a_{23}], [h_{a_{12}}(s_2), h_{a_{32}}(s_2)]), \\ &(A_{k_3}(H_3), s_3, [a_{31}, a_{32}], [h_{a_{13}}(s_3), h_{a_{23}}(s_3)]). \end{aligned} \tag{7}$$

Note that this is more complicated than the scheme in section 4. Instead of giving the keys k_i to the other two players, we have instead shared them among all three players, so no single component has access to any of the three keys used for quantum authentication. In section 4, we were able to use the fact that the quantum register attacked by the adversary must be the same as the classical register attacked, so it is only necessary to protect information about one of the keys k_i, not all of them. With the extra flexibility granted the adversary by being able to attack multiple registers, it is more straightforward to protect all n keys with the classical ETSS.

We are now ready for our main result. Let $H'_1 \otimes H'_2 \otimes ... \otimes H'_n$ be the coding space of the new code

$$\mathcal{Q}'|\psi\rangle \in H'_1 \otimes H'_2 \otimes ... \otimes H'_n$$

Theorem 2 *If A_k is a* QAS *secure with error ϵ, Q is a non-degenerate stabilizer code with distance d, and $h_a(\cdot)$ is a classical authentication scheme with error ϵ, then $\mathcal{Q}'$ is an approximate quantum error-correcting code correcting $d-1$ arbitrary errors with error at most $2n^2\epsilon$.*

5.1 Reconstruction

The reconstruction procedure is similar to that for the previous protocol, but slightly more involved, since we must verify the classical authentications as well. Rather than breaking the procedure into different cases, in this version of the protocol, we can systematically go through four steps: First, verify the classical authentications and discard any invalid classical share. Second, reconstruct the keys k_i. Third, verify and decode the quantum authentications. Fourth, discard any invalid quantum register and reconstruct the encoded quantum state.

1. Verify classical authentications:
   For each s_i, consider it valid if at least half its authentications are correct according to $a_{ji}, j \neq i$. Discard any share s_i which is not valid.
2. Reconstruct the keys k_i:
   Up to $d-1$ shares s_i can have been discarded in the first stage, so at least $n - d + 1 \geq n/2 + 1 > d$ shares remain. Use these to reconstruct $(k_1, \ldots, k_n)$. If the remaining shares are not all consistent with a single value of the secret, Bob aborts and outputs the quantum state $|0\rangle$.
3. Verify and decode the quantum authentications:
   Use the key k_i to verify and decode the quantum authentication $A_{k_i}(H_i)$.

4. Reconstruct the encoded quantum state:
   Discard any registers which failed the quantum authentication, and use the remaining registers to reconstruct the valid codeword as $c|\psi\rangle \in H_1 \otimes \ldots \otimes H_n$ using the erasure recovery algorithm. (At most $d-1$ have been discarded.) If the remaining registers are not consistent with a single quantum codeword, Bob aborts and outputs the quantum state $|0\rangle$.

We prove this assuming the original QECC $\mathcal{Q}$ is a nondegenerate CSS code (which is sufficient to demonstrate that AQECCs exist correcting up to $(n-1)/2$ errors), but the proof can easily be extended to an arbitrary stabilizer code.

Proof (of Theorem 2). If no errors occurred, the above procedure will exactly reconstruct the original encoded state. We need to show that it still approximately reconstructs the state when there are up to $d-1$ arbitrary errors in unknown locations. Let B be the set of registers attacked by the adversary, and let $A = [n] \setminus B$ be the registers held by honest players.

The intuition for the proof is simple. With high probability, the authentication keys will be reconstructed correctly; conditioned on that event, all components of the QECC which pass the authentication test should be "close" to the encoding of $|\psi\rangle$ restricted to those positions, and applying erasure correction should yield a state very close to $|\psi\rangle$. Formalizing this intuition is more delicate than it would be if the data involved were classical. The quantum version of the statement "such-and-such event holds with probability $1-\epsilon$" is "the state of the system has fidelity at least $1-\epsilon$ to the subspace such-and-such." The problem lies in the fact that the union bound from ordinary probability, which is the basis of the intuition outlined above, does not always hold in the quantum world. Our solution follows the lines of the "quantum to classical reductions" in [14, 9]. We define a set of "target" subspaces whose projectors commute (in other words, there exists a single basis of the state space in which all the projectors are diagonal), and show that the system lies close to each of these target subspaces. For commuting subspaces, the union bound does hold: if the system has high fidelity to each of the subspaces, then in fact it has high fidelity to their intersection. To complete the proof it is sufficient to show that for states in the intersection, the initial input $|\psi\rangle$ is reconstructed exactly.

The first step is to take care of the classical component of the encoding (composed of the shares s_i, classical authentication keys a_{ij} and tags $h_{a_{ij}}(s_j)$). We rely on three observations. First, we may assume w.l.o.g. that the recovery procedure measures all the classical components in the computational basis before doing any processing; thus, the state received by the reconstructor Bob is a mixture (not a superposition) over different bit strings which he might be sent instead of the original ones. Second, the classical information held by the adversary is statistically independent of $\boldsymbol{k} = (k_1, ..., k_n)$, the vector of quantum authentication keys. (This follows from the fact that any t of the shares $s_1, ..., s_n$ are independent of the shared secret.) Third, any classical authentication tags changed by the adversary will be rejected by Bob with probability at least $1-\epsilon$.

We define our first target subspace S_0 by the statement "the keys $\boldsymbol{k}$ reconstructed by Bob are equal to the original keys." This statement can fail only

if some tag changed by the adversary is accepted by Bob, and by a (classical) union bound this can occur with probability at most $tn\epsilon < n^2\epsilon$. The fidelity to S_0 is thus at least $1 - n^2\epsilon$.

We now look at what happens within the subspace S_0. Consider the following set of measurements which might be performed by Bob after verifying the authentications, but before applying erasure correction to the code. We assume for simplicity that the adversary holds the wires $B = \{1, ..., t\}$, and the wires $A = \{t+1, ..., n\}$ are untouched.

- For each register $i \in [n]$, $|\text{REJ}_i\rangle\langle\text{REJ}_i|$ measures whether or not Bob rejected the authentication of the i-th quantum system (correspondingly, $|\text{ACC}_i\rangle\langle\text{ACC}_i|$ measures whether or not Bob accepts).
- We use the fact that the quantum error-correcting code is a nondegenerate CSS code. The code can be defined by a sequence of parity checks performed in two bases: the standard computational basis and the rotated Fourier (or "diagonal") basis. We assume there are r independent parity checks in the rotated basis and s independent parity checks in the standard basis. Denote by V the linear space of parity checks satisfied in the computational basis, and by W the corresponding set for the Fourier basis. If the QECC code has distance at least $t+1$, then there is a basis $v_1, ..., v_s$ of V such that, for any $i \in B$, position i is only in the support of v_i. Same for W: there is a basis of parity checks $w_1, ..., w_r$ such that only w_i involves the i-th component of the code for $i \in B$. We denote by Π_{v_i}, Π_{w_i} the corresponding projectors (that is, Π_{v_i} preserves the supspace in which the parity check v_i is satisfied).

The sets of projectors $\{|\text{REJ}_i\rangle\langle\text{REJ}_i|\}_{i\in[n]}$, $\{\Pi_{v_i}\}_{i\in[s]}$ and $\{\Pi_{w_i}\}_{i\in[r]}$ all commute with each other. The only possible interaction comes from the fact that the operators $\{\Pi_{v_i}\}$ and $\{\Pi_{w_i}\}$ operate on the same space, but they commute by definition of CSS codes. We may ignore projectors with indices $i > t$ since they correspond to checks which will always be passed within the subspace S_0: Therefore the system will have fidelity 1 to the subspaces defined by $\{\Pi_{v_i}\}$ and $\{\Pi_{w_i}\}$ for $i > t$.

We would like to claim that, whenever Bob accepts the set R of registers, R satisfies all the parity checks restricted to R. We can quantify this as follows: for all i between 1 and t, the system should lie in the subspace defined by

$$P_i = (\Pi_{v_i}\Pi_{w_i} \otimes |\text{ACC}_i\rangle\langle\text{ACC}_i|) + (I \otimes |\text{REJ}_i\rangle\langle\text{REJ}_i|). \tag{8}$$

where I is the identity operator. The security of the quantum authentication scheme, and the fact that the adversary doesn't learn anything about the keys from the classical secret sharing, imply that the fidelity to each of these subspaces is at least $1 - \epsilon$ (note: this requires the quantum authentication scheme to be secure even when composed up to t times). For $1 \leq i \leq t$, we can define the subspaces $S_1, \ldots, S_t$ corresponding to the projectors $P_1, \ldots, P_t$. By a union bound, the state of the whole system has fidelity at least $1 - n^2\epsilon - t\epsilon$ to the intersection $S = \bigcap_{i=o}^{t} S_i$. In words, S is the space of states for which Bob

reconstructs the correct authentication keys, and for which the set of registers accepted by Bob satisfies all the parity checks restricted to that set.

It remains to prove that within the space S, Bob will always recover the input state $|\psi\rangle$ exactly. We may assume w.l.o.g. that Bob will measure all n of the registers which indicate whether the authentication failed or not in the basis $\{|\text{REJ}\rangle, |\text{ACC}\rangle\}$. Thus, the global state may be seen as a mixture over possible sets of registers accepted by Bob. If Bob also performs the measurements P_i, he will, with probability at least $1 - n^2\epsilon - t\epsilon$, find that the state actually satisfies all parity checks restricted to the set R of registers he accepts.

When this occurs, it then follows that applying erasure correction to R yields the same result as if we had used only registers untouched by the adversary. For a detailed proof of this fact, we refer the reader to Proposition 2.2 in [9]. The intuition behind it is straightforward: Suppose s registers are discarded, leaving up to $t - s$ registers attacked by the adversary. But because $s + (t - s) < d$, the QECC can both correct s erasures and detect an additional $t - s$ errors, so the adversary is unable to reach any state in S except the correct input state $|\psi\rangle$. We can conclude that Bob recovers a state ρ with fidelity at least $1 - 2n^2\epsilon$ to ψ, as desired.

5.2 Specific Constructions and Parameters

As mentioned above, it is natural to instantiate our construction using the polynomial codes (quantum Reed-Solomon codes) of Aharonov and Ben-Or [1]. These are nondegenerate CSS codes over an alphabet of size q whenever q is a prime power and greater than $n - 1$. For any $t < n/2$, one can find a $[[n, n - 2t, t + 1]]_q$ code (i.e. which encodes $(n - 2t) \log q$ qubits and has distance $t + 1$). This means that to encode $\ell > n$ qubits, each component of the code will consist of $\ell/(n - 2t)$ qubits. The components of the approximate QECC then consist of $\ell/(n - 2t) + O(\log(\frac{1}{\epsilon}))$ qubits and $CC(2\ell/(n - 2t) + O(\log(\frac{1}{\epsilon})), \epsilon, t)$ bits (where $CC()$ is the share size of the classical ETSS).

For $2t < n-1$, we can modify the ETSS above to get shares of size $O(n \log(\frac{1}{\epsilon}))$ $+ \ell/(n - 2t)$. Putting these constructions together, we can get quantum codes where each register contains $O(n(\ell/(n - 2t) + \log(\frac{1}{\epsilon})))$ qubits.

An immediate improvement can be made to these parameters by noting that, for any distance d nondegenerate stabilizer code, including the polynomial codes used here, the state of any $d - 1$ registers is maximally entangled with the remaining registers. Therefore, as noted in section 2, a much shorter classical key suffices for quantum authentication. In particular, a classical key of length $O(\log \ell + \log(\frac{1}{\epsilon}))$ is sufficient to authenticate ℓ EPR halves. This leads to an approximate quantum code where each component consists of $\ell/(n-2t)+O(\log(\frac{1}{\epsilon}))$ qubits and $CC(n \log(\frac{1}{\epsilon}), \epsilon, t)$ bits (when $\epsilon < 1/\ell$). This gives a total size of $\ell/(n - 2t) + O(n \log(\frac{1}{\epsilon}))$.

Corollary 3 (to Theorem 2) *For $t < n/2$, there exists an approximate QECC correcting any t errors with error ϵ, where each component consists of $O(\ell/(n -$*

$2t) + n \log(\frac{1}{\epsilon})))$ *qubits. When* $n = 2t + 1$*, we get components of size* $O(\ell + n \log(\frac{1}{\epsilon}))$.

6 Discussion and open questions

We have constructed quantum error correcting codes that are capable of correcting general errors when up to half the registers are affected. This contrasts considerably with known upper bounds that limit a QECC to correcting errors on less than one-fourth of all registers. The price for being able to violate this bound is that we only correct the state approximately; however, we do so with exponentially good fidelity.

In general, extrapolating from exact performance of a quantum task to approximate performance is dangerous, but possible. Factors of the dimension may arise, and since the dimension is exponential in the number of qubits, dramatically different behavior becomes possible. This phenomenon is likely behind the performance of our codes, and suggests that high-fidelity AQECCs are only possible when working in high dimension.

Our codes instead consist of a small logical subspace and large registers containing both quantum and classical information. As such, they are not so useful for practical problems in quantum error correction, but do serve as an interesting in-principle demonstration of the potential power of approximate error correction. In addition, they act as quantum ETSS schemes, and may be a useful stepping stone towards building VQSS and MPQC with a large number of cheaters. Any such construction must be more complex, however, to take account of dishonest senders and receivers, and to allow the participants in the protocol to alter a state in the correct way without altering it in any unapproved manner. Indeed, it remains possible that the prior bound of $n/4$ cheaters does in fact restrict VQSS and MPQC; however, we have shown here that the existing proof of that bound does not apply to VQSS and MPQC protocols which only guarantee approximate reconstruction of the quantum state.

References

1. D. Aharonov and M. Ben-Or. Fault tolerant quantum computation with constant error rate. Preliminary version in *Proc. 29th ACM Symp. on Theory of Computing*, 1997. Submitted to SIAM J. Comp., June 1999.
2. H. Barnum, C. Crépeau, D. Gottesman, A. Tapp, and A. Smith. Authentication of quantum messages. In proceedings of The 43rd Annual IEEE Symposium on Foundations of Computer Science (FOCS'02), November 16 - 19, 2002 Vancouver, BC, Canada, pages 449–458. Also Quantum Physics, abstract quant-ph/0205128, 22 pages, May 2002.
3. H. Barnum, E. Knill and M. A. Nielsen, "On Quantum Fidelities and Channel Capacities," quant-ph/980901, IEEE Trans.Info.Theor. 46 (2000) 1317-1329.
4. C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, "Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels.", Phys. Rev. Lett. 76 (1996) 722-725, Quantum Physics, abstract quant-ph/9511027.

5. S. Cabello, C. Padró, G. Saéz. Secret Sharing Schemes with Detection of Cheaters for a General Access Structure. *Designs, Codes and Cryptography*, 25(2): 175-188 (2002).
6. Richard Cleve, Daniel Gottesman, Hoi-Kwong Lo. How to share a quantum secret. *Phys.Rev.Lett.* 83, p. 648–651, 1999.
7. R. Cramer, I. Damgård, S. Dziembowski, M. Hirt and T. Rabin. Efficient Multiparty Computations Secure Against an Adaptive Adversary In *Advances in Cryptology — EUROCRYPT 1999*.
8. R. Cramer, I. Damgård, S. Fehr. On the Cost of Reconstructing a Secret. In *Advances in Cryptology — CRYPTO 2001*.
9. C. Crépeau, D. Gottesman, and A. Smith. Secure multi-party quantum computation. In Proceedings of 34th Annual ACM Symposium on Theory of Computing, May 19-21, 2002, Montréal, Québec, Canada. ACM, 2002, pages 643–652.
10. P. Gemmell and M. Naor. Codes for interactive authentication. In D. R. Stinson, editor, *CRYPTO*, volume 773 of *Lecture Notes in Computer Science*, pages 355–367. Springer, 1994.
11. D. Gottesman, "An Introduction to Quantum Error Correction.", Quantum Physics, abstract quant-ph/0004072, 15 pages, talk given at AMS Short Course on Quantum Computation.
12. P. Hayden, D. Leung, D. Mayers. Universally composable quantum authentication. In preparation.
13. P. Hayden, D. Leung, A. Winter and P. Shor. Randomizing quantum states: Constructions and applications. *Commun. Math. Phys.* 250(2): 371-391, 2004.
14. Hoi-Kwong Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283(5410):2050 2056, 26 March 1999.
15. D. W. Leung, M. A. Nielsen, I. L. Chuang, and Y. Yamamoto. Approximate quantum error correction can lead to better codes. Phys.Rev. A56 (1997) 2567–2573, quant-ph/9704002.
16. R. J. McEliece and D. Sarwate. On sharing secrets and Reed-Solomon codes. *Comm. ACM* 24, 1981, 583–584.
17. M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
18. J. Oppenheim and M. Horodecki. How to reuse a one-time pad and other notes on authentication, encryption and protection of quantum information. E-print quant-ph/0306161.
19. T. Rabin and M. Ben-Or. Verifiable Secret Sharing and Multiparty Protocols with Honest Majority. In *Proc. of STOC 1989*, p. 73–85.
20. A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, 1979.
21. B. Schumacher, M. D. Westmoreland Approximate quantum error correction. E-print quant-ph/0112106, 2001.
22. A. Smith. Quantum secret sharing for general access structures. E-print quant-ph/0001087, 2000.
23. K. Srinathan, Arvind Narayanan and C. Pandu Rangan: Optimal Perfectly Secure Message Transmission. *Advances in Cryptology — CRYPTO 2004*.
24. W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned", *Nature* 299, 802, 1982 .